Session 617

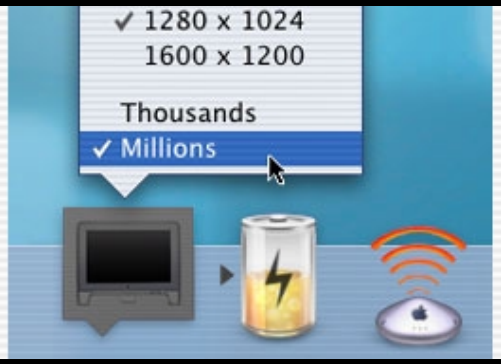
WebObjects & Security

David Neumann
ObjectWare Engineer

Introduction

- Protecting privacy
- Protecting resources
- Authentication
- Persistent data integrity
- Message integrity
- Access control

Keeping It Private



Using SSL in WebObjects

- WO generates partial URLs by default

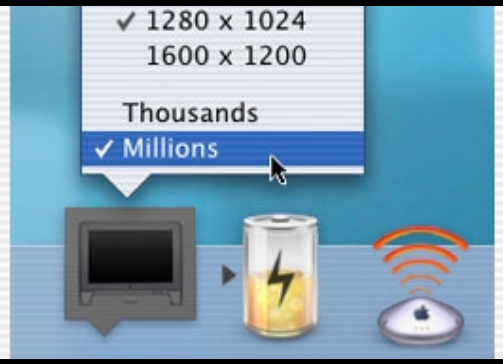
  /cgi-bin/WebObjects/App.woa/wo/F00000EXSA/1.2

- To force SSL you need to:
  - Access your application from a secure link initially, **or**
  - Force WO to generate full URLs

  https://wosite.com/cgi-bin/WebObjects/App.woa/wo/F00000EXSA/1.2

Demo

Using a Custom Component to Generate Absolute URLs



David Neumann
ObjectWare Engineer

SSL Access Via Redirection

- Override **appendToResponse**
  - Works regardless of how they got here (DA or CA)
- Let the page determine if it has to be private
- If so, check if coming in over https://
- If not, redirect back to the page
  - Don't double generate page
  - Don't double invoke the same action

Detecting SSL

- It's tricky; depends on your web server
  - Is there a header named "**HTTPS**" set to "**ON**"?
  - If not, is the server port (header named "**SERVER_PORT**" or "**x-webobjects-server-port**") set to "**443**" ?
  - Other criteria?

Demo

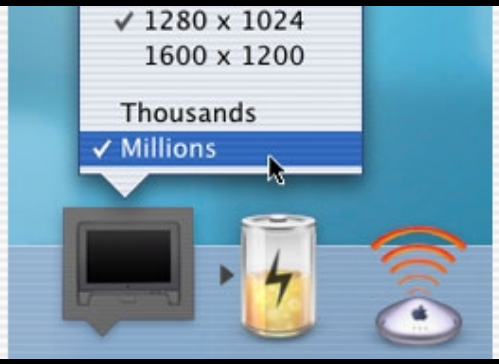
SSL Redirect Without Side Effects

David Neumann
ObjectWare Engineer

Session Hijacking

- What is it?
  - Only care if there's a session AND the user has authenticated to that session
  - SSL alone not enough to protect you
  - The over-the-shoulder attack
- One solution…
  - Emit a cookie specific to a user's session
  - If the cookie is missing or doesn't belong to the session, access to the application is rejected

Protecting WO Resources



Page Generation Protection

- You let the page get created, but don't let it generate a response
- Override WOComponent's **appendToResponse()**
  - Not necessarily OK to go to CAs or DAs destination
  - Prevent page display no matter how page is accessed
    - Initial app access, DA, or CA

Page Creation Protection

- You override **pageWithName()** on the Application to prevent page creation
  - Might have a list of forbidden page names

Pros/Cons

A. Page creation protection

1. (+) Prevents side-effects in the page constructor from executing unless you are logged-in
2. (-) Can't affect pages after they are created
3. (-) Your code would have to tolerate getting a different page than expected

B. Page generation protection

1. (+) Allows that page to decide what to do
   1. You might use the same page in different contexts
2. (+) Action code can remain unaltered
3. (-) You have to make sure that constructor code does not require authentication

- I'd argue that B.3 is easier than A.3

DirectAction Protection

- Override **performActionNamed()** to prevent DA invocation
  - DAs can be accessed from anywhere
    - Whether you generate page or not (can't hide them)
  - Protecting **appendToResponse()** does not prevent the DA from executing
    - . . .But does hide the result

Backtracking

- Don't really apply to DAs, only CAs
  - If you shouldn't backtrack to a DA, then it probably shouldn't be a DA
- Can detect with context ID
- Can override **invokeAction()** on pages where backtracking not allowed
  - Can abort call to **super.invokeAction()** if backtrack detected
  - Results in merely page refresh

Demo

Page Generation Protection / DA Invocation Protection

David Neumann
ObjectWare Engineer

Authentication

David Neumann
ObjectWare Engineer

When to Login

- Front Gate
- On demand
- Prompt for login on WOSession timeout

Front Gate Protection

- Usual form
- Somewhat unfriendly
- Users cannot vector in

Browse Then Demand

- Allow surfing until login required
- Two ways to go…
  - Go to login page, and re-navigate to protected page
  - Prompt for login then immediately access protected resources
- Combine with the resource protection schemes

Demo

On-Demand Login

(Backtrack Detection and Prevention)

David Neumann
ObjectWare Engineer

Authentication Methods

- HTML page
- HTTP panel
- Client Certificates
- Biometric
- Combinations
- Other…

Using HTTP Challenge Panel

- You must emit certain status and headers in responses
- You must look for certain headers in requests
- Your web server might not work
- You have to parse Base64-encoded data

Using HTTP Challenge Panel

- Your web server must use an interface that passes the "authorization" header to the WOAdaptor
  - PWS/CGI and Netscape/CGI do not
  - Netscape/NSAPI and Apache/module do
- What's the realm!?
  - A name associated with resources behind the web server
  - Your application and the web server might use the same realm name
  - Can provides element of SSO for static HTML and WOApps

Using Client-side Certificates

- Need special www server setup
- Credentials are a token
  - Your private/public key pair
  - Can be stored on hardware device
- Can provide SSO for WOApps and static HTML

Using Client-side Certificates

- Sort of the inverse of regular login
  - SSL proves you are who you say
  - The application decides if the person is in the system
- Need to modify WOAdaptor source
  - To request certificates from interface if needed
  - To pass the client certificates on to WOApp as header

Verifying Certificates

- See if the certificate has been revoked
  - Download a CRL from CA's web server
  - Get status online using VA's OCSP server
- Microsoft Example…

Using Biometrics

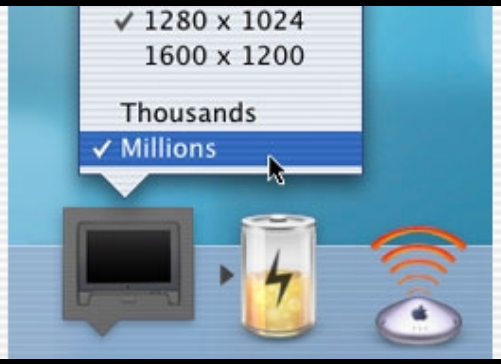
- Something about you…
  - Physical imaging
    - Thumbprint, palmprint, retina, face
  - Your voice
  - How you type
- Combination with password

Recording Login Failures

- Write out row for failed access attempts
  - Allows for auditing reports
  - Required for multiple instances
- Fetch against table and do count on attempts
  - By username, IP, and/or cookie (in last X seconds)
- Use count to drive counter measures
  - Emailing admin
  - Disabling an account
  - Disabling access from certain IP

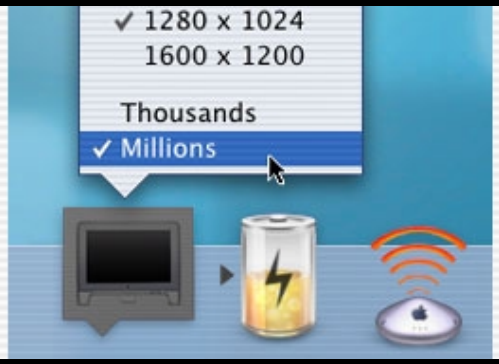
Demo

Denying Login Due to Intrusion Attempts



David Neumann
ObjectWare Engineer

Persistent Data Integrity



Hashing

For Ex: Passwords

- Don't ever store passwords in the clear
- Storing a password hash is better
- Hash incoming passwords and compare to the stored hash
- If someone cracks your DB, the "passwords" are useless (sort of)
  - BTW: What's a hash?

Encryption

For Ex: Credit Card Numbers

- If item must be recovered (and not just equality tested)
- Use special accessors to do this transparently
- You might let a hardware device perform the actual encryption/decryption (PKCS#11)
  - The key never leaves the device (gotta hack the device not just the computer)
    - Chrysalis-ITS
    - nCipher

Demo

Using Hashes and Encryption

David Neumann
ObjectWare Engineer

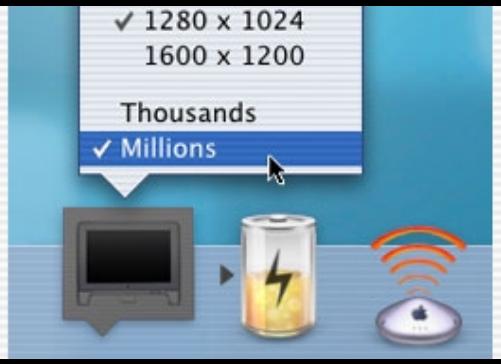
Signatures and Timestamps

For Ex: Documents

- Store hashes of docs with stored doc
  - Easy to alter doc and rehash
- Store digitally signed docs
  - Can't alter doc then fake a rehash
- Embed digital timestamp with signed doc
  - Now we have proof when it was created
- Format for the doc is ideally XML
  - Standard DTD exists

http://www.oasis-open.org/cover/dridtd-19990119.html

Messaging Integrity



B2C Digital Signatures

- Clients require a browser plug-in or applet
- Example applications
  - Employee forms processing
  - Brokerage enrollment
  - Paperless workflow with authorization

B2B Digital Signatures

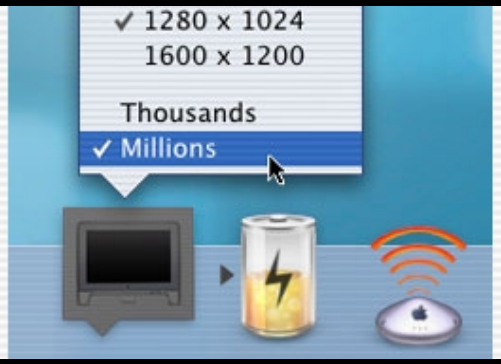
- When machines send and receive digitally signed messages
- Ex: DropShip order, PO, any EDI message

B2B Infrastructure in WO

- WODirectActions
  - Turn WOApps into services
- WOMessage
  - Programmatically send WORequests to remote apps; read WOResponses
- XML management
  - Generate XML sent over the net
  - Interpret XML received

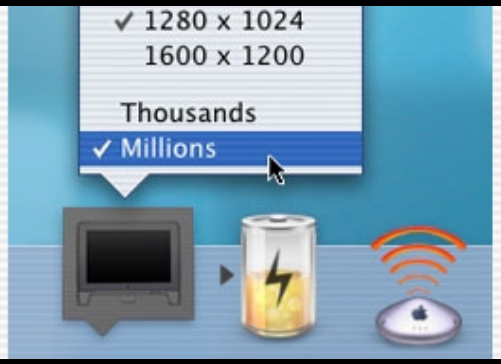
Demo

B2B Example of Signing/Validating XML



David Neumann
ObjectWare Engineer

Access Control



Access Control

- Degree of access granted after they login
- Given object A (an EO, say), can user B:
  - See it?
  - Edit it?
  - Do something else with it?
- Access depends on the state of both A and B

Access Control

Techniques

- Have all your EOs implement an interface like this:

```
public boolean canShow(User usr);
public boolean canEdit(User usr);
public Object valueForKeyUser(String key, User usr);
public void takeValueForKeyUser
(Object val, String key, User usr);
```

Access Control

Techniques

- Implementation of SecuredEO might be:

```
public boolean canShow(User usr){
    if(usr.equals(creator()))
        return true;
    else if(owners().containsObject(usr))
        return true;
    return false;
}

public boolean canEdit(User usr){
    return canShow(usr);
}
```

Apply It to the UI

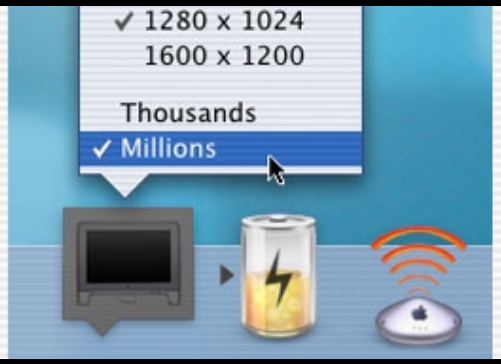
- Use WOConditionals to hide edit controls for EOs that can be seen but not edited
- Filter non-readable EOs out of result sets
- Use group membership to hide/show areas of the page

Complex Access Control

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Demo

Integrating Java's ACL impl for Use With EOs



David Neumann
ObjectWare Engineer

Summary

- Protecting privacy
  - SSL, components, redirection, detection
- Protecting resources
  - WO request handling overrides
- Authentication
  - Gather credentials via HTML page, certs, panels, etc.

Summary

- Persistent data integrity
  - Using hashing and encryption
- Message integrity
  - Signing/validating request/responses
- Access control
  - Using ACLs with EOs

For More Information

Get the FAQ
http://www.rsa.com/

Leading VA
http://www.valicert.com/

Leading CA
http://www.verisign.com/

Signing Plug-in
http://www.adobe.com/

HSM Vendor
http://www.ncipher.com/

Dig Receipt
http://www.oaisi-open.org/

Dig Timestamp
http://www.verisign.com/

WebObjects Lab

- Located downstairs in Room K
- Lab hours
  - Monday 12:00pm–6:00pm
  - Tuesday 10:30am–6:00pm
  - Wednesday 10:30am–6:00pm
  - Thursday 10:30am–6:00pm
  - Friday 10:30am–3:30pm

☑ Vote for WebObjects as Best App Server

http://developer.apple.com/webobjects

Roadmap

618 Optimizing WebObjects Applications	Room A1 **Fri., 2:00pm**
FF111 Feedback Forum: WebObjects	Room A1 **Fri., 3:30pm**

Who to Contact

Toni Trujillo Vian
Director, WebObjects Engineering
webobjects@apple.com

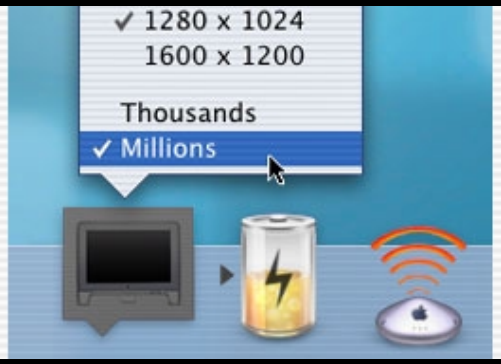
Bob Fraser
WebObjects Product Manager
webobjects@apple.com

iServices Consulting, Integration, Training & Certification
(800) 848-6398
iservices@apple.com

For more information:
www.apple.com/webobjects
developer.apple.com/webobjects
www.apple.com/iservices
www.info.apple.com/webobjects

Subscribe to:
webobjects-announce@apple.com

Q&A



Bob Fraser
WebObjects Product Manager
webobjects@apple.com

http://developer.apple.com/events/urls.html

WWDC
Worldwide Developers Conference 2001